

Amendments to the Claims:

This listing of claims will replace, without prejudice, all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A ~~home security~~ system for monitoring an ~~home~~ environment comprising:

an Internet browser connectable to an extranet;

an extranet located external to said ~~home~~ environment and accessible via said Internet browser;

a communications server located in said extranet and adapted to interconnect on demand with one of a series of connection gateways located in predetermined ~~home~~ environments; and

a connection gateway located in said ~~home~~ environment to serve as a user interface for the control or monitoring of the operation of at least one service in said ~~adapted to control and/or monitor the operation of at least one security device in said home~~ environment;

wherein upon accessing a predetermined address by said Internet browser on said extranet, said communications server creates a new connection to a predetermined one of said connection gateways to control or monitor the operation of said service, with said connection gateway subsequently serving pages directly to said internet browser displaying the state of operation of said service ~~connects to a predetermined one of said connection gateways to control and/or monitor the operation of said security device.~~

2. (New) A system as claimed in claim 1, wherein said service includes a monitoring device located within said environment.

3. (New) A system as claimed in claim 1, wherein said communication server utilizes a telecommunications network to interconnect with said connection gateway.

4. (New) A system as claimed in claim 1, wherein said extranet forms part of the Internet and said communications server is located within the local telephone call radius of the environment, thus providing lowest cost PSTN access from or to the environment.

5. (New) A system as claimed in claim 1, wherein authentication to access said extranet is required only once per Internet browser session
6. (New) A system as claimed in claim 1, wherein publicly accessible HTML pages are additionally provided for each user of said system providing details of the current status of the environment of said user.
7. (New) A system as claimed in claim 1, wherein said extranet provides a user premises e-mail facility, and automatically raises connection in a pre-programmed fashion to said connection gateway and transfers user e-mail to said connection gateway.
8. (New) A system as claimed in claim 1, wherein said the Internet browser runs on an Internet access device which includes a smart card reader and associated user smart card which provides authentication details and URL corresponding to said environment.
9. (New) A system as claimed in claim 8, wherein said smart card also facilitates global access to the Internet for access of said extranet, and optionally additionally tracks connections for expensing.
10. (New) A system as claimed in claim 1, wherein the Internet access device is a computer, WebPhone, Portable digital assistant, or mobile phone with web browsing capability.
11. (New) A system as claimed in claim 1, wherein the connection gateway detects a fax and stores the fax.
12. (New) A system as claimed in claim 1, wherein the connection gateway is in a tamper proof enclosure, and operates without mains power.
13. (New) A system as claimed in claim 1, wherein the connection gateway is tamper proof, and triggers an alarm and relays alarm to the provider network in case of attempted tampering.

14. (New) A system as claimed in claim 1, wherein the connection gateway acts as a hub and Internet connection mechanism for connected devices including information appliances and said devices located in said environment.

15. (New) A system as claimed in claim 1, further comprising a control terminal interconnected to said connection gateway, said control terminal comprising a display incorporating a touch screen and a running web browser.

16. (New) A system as claimed in claim 15, wherein the control terminal is equipped with biosensor, for access authentication of a local user in said environment to said connection gateway.

17. (New) A system as claimed in claim 15, wherein the control terminal is connected to said connection gateway in a wireless manner.

18. (New) A system as claimed in claim 17, wherein the control terminal is powered by rechargeable batteries, allowing the control terminal mobility within the range of wireless transmitters attached to the user premises network in said environment..

19. (New) A system as claimed in claim 15, wherein the control terminal is of a reduced handheld size, so that can operate as universal premises remote control

20. (New) A system as claimed in claim 15, wherein the control terminal includes a digital camera, microphone and speaker, and video conferencing software, thus allowing the control terminal to be used as a videophone, through a standard browser interface.

21. (New) A system as claimed in claim 15, wherein the control terminal includes a personal computer (PC) equipped with a user premises network connection, wherein said PC runs a browser accessing a URL corresponding to said connection gateway.

22. (New) A system as claimed in claim 15, wherein the control terminal includes a set top box connected to a television and executes a web browser.

23. (New) A system as claimed in claim 15, wherein the control terminal includes a smartcard reader for e-commerce transactions over said extranet.
24. (New) A system as claimed in claim 1, wherein at least one of said devices comprises a digital security camera having an image capture and compression functionality and an interconnection to said connection gateway.
25. (New) A system as claimed in claim 24, wherein said camera includes motion detection and image significance algorithms which run in said camera, and filter input so that only detected motion input is compressed and sent through said connection gateway to said extranet.
26. (New) A system as claimed in claim 1, wherein at least one of said devices includes an external access control mechanism to said environment.
27. (New) A system as claimed in claim 1, wherein at least one of said devices includes a reader for an RF tag embodied in keyfob or other device that is used for user authentication.
28. (New) A system as claimed in claim 1, wherein at least one of said devices includes a smartcard reader for user authentication.
29. (New) A system as claimed in claim 1, wherein said connection gateway provides support for at least one of the HomePnP, Bluetooth, HomeRF, Hiperlan and HAVi standards for network communication and appliance control.
30. (New) A system as claimed in claim 28, wherein the smartcard includes a biosensor attached to the substrate of the smart card and interconnected with a circuit embedded in smartcard to authenticate user before the smartcard will operate.
31. (New) A system as claimed in claim 1, wherein said connection gateways form nodes of a distributed computing environment that may be allocated by said extranet on a demand basis.

32. (New) A system for providing information access across at least two networks, the system comprising:

- a first network having a first network access controller;
- a second network having a second network access controller;
- a user access browser located on said first network for locating and examining information on said first and second networks by means of network address locators;
- wherein when a predetermined location on said network is accessed, said first network access controller initiates the establishment of a network connection to said second network access controller so as to provide for the temporary interconnection of said first network to said second network, said system thereby providing a seamless access to information stored on said second network from said user access browser.

33. (New) A system as claimed in claim 32, wherein said network address locators comprise Universal Resource Locators.

34. (New) A security system for monitoring an environment comprising:

- an extranet located external to said environment;
- storage means forming part of said extranet;
- at least one communications server located in said extranet and adapted to interconnect on demand with one of a series of connection gateways located in predetermined environments;
- a connection gateway located in said environment adapted to control and/or monitor the operation of at least one security device in said environment; and
- a security device activating a security condition upon the occurrence of a predetermined event;
- wherein, upon the occurrence of said predetermined event, said security device notifies said connection gateway and transfers event information on said predetermined event to said connection gateway and said connection gateway establishes an interconnection with said communications server and transfers said event information via said communications server to said storage means for later interrogation by a user of said security system.

35. (New) A system as claimed in claim 34, wherein said security device includes alert conditions which are forwarded to said connection gateway, wherein it is qualified with a pre-programmed enable, and if the result is TRUE, an alarm event is generated, whereupon

said connection gateway establishes a connection with one of said communications servers, and surveillance data related to said alarm event is uploaded to said extranet for secure storage accessible upon interrogation by a user.

36. (New) A system as claimed in claim 35, wherein photos of authorised occupants of said environment are accessible from said extranet and are accessed upon an alarm event and cross referenced with surveillance data to ascertain whether a true alarm condition has been raised.

37. (New) A system as claimed in claim 35, wherein the connection gateway incorporates a user programmed phone call answer strategy, including delayed answer, and upon answering said phone call, optionally detects a voice call, in which case it records a compressed version of the voice call for later retrieval by the user, thus operating in answering machine mode.

38. (New) A system as claimed in claim 37, wherein upon answering an incoming call, the connection gateway raise a connection to a communications server, and sends an indication to the user of said security system of the receipt of a recorded message.

39. (New) A system as claimed in claim 34, wherein said connection gateway sends a recorded compressed voice message to a communications server for storage on said extranet for forwarding to a user of said environment.

40. (New) A system as claimed in claim 34, wherein the connection gateway provides an indication of messages received on a HTML page accessible by a user of said home environment.

41. (New) A system as claimed in claim 34, wherein said connection gateway is programmable to allow different response mechanisms to differing classes of alert event.

42. (New) A system as claimed in claim 34, wherein said connection gateway contains connection details for preferred and secondary communication servers on said extranet, so that if a first communication server does not respond, other communication servers may be contacted until successful connection is achieved.

43. (New) A system as claimed in claim 34, wherein user data storage on said extranet for storing event data associated with said environment is allocated virtually.
44. (New) A system as claimed in claim 34, wherein said user data storage on said extranet is allocated redundantly, ensuring integrity of stored surveillance data.
45. (New) A system as claimed in claim 34, wherein said extranet includes a user contact database which includes preferred contact methods, allowing automatic contact mechanisms to be associated with alarm condition, including use of e-mail, pager, computer generated voice message through telephone, requesting response, or after a specified timeout has elapsed, security action.
46. (New) A system as claimed in claim 1, wherein said environment is a home environment.
47. (New) A system as claimed in claim 1, wherein said environment is a commercial environment
48. (New) A system as claimed in claim 1, wherein said environment is an industrial environment
49. (New) A system as claimed in claim 1, wherein the at least one service includes a security monitoring service.
50. (New) A system as claimed in claim 1, wherein the at least one service includes a video surveillance service
51. (New) A system as claimed in claim 1, wherein the at least one service includes an automation and control service
52. (New) A system as claimed in claim 1, wherein the at least one service includes a utility metering service

53. (New) A system as claimed in claim 1, wherein the at least one service includes an energy management service

54. (New) A system as claimed in claim 1, wherein the at least one service implements monitoring or control of a plurality of devices connected to at least one network interconnected with the connection gateway.

55. (New) A system as claimed in claim 1, where the internet browser is on mobile phone.

56. (New) A system as claimed in claim 1, wherein said the Internet browser runs on an Internet access device which includes a smart card reader and associated user smart card which provides authentication to access said predetermined address to create a connection to said environment.

57. (New) A system as claimed in claim 1, wherein the connection gateway is embodied in a security camera.

58. (New) A security system for monitoring an environment comprising:

an extranet located external to said environment;

storage means forming part of said extranet;

a connection gateway located in said environment adapted to control and/or monitor the operation of at least one security device in said environment; and

a security device activating a security condition upon the occurrence of a predetermined event;

wherein, upon the occurrence of said predetermined event, said security device notifies said connection gateway and transfers event information on said predetermined event to said connection gateway and said connection gateway establishes an interconnection with said communications server and transfers said event information via said communications server to said storage means for remote storage for later interrogation by a user of said security system.